IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
(Greenbelt Division)

NATIONAL ASSOCIATION OF BLACK ACCOUNTANTS, INC., Plaintiff, v. **WHITE INVESTMENTS LLC AND JOHN DOE NOS. 1-100,** Defendants.	Case No.

COMPLAINT

Plaintiff NATIONAL ASSOCIATION OF BLACK ACCCOUNTANTS, INC. ("NABA" or "Plaintiff"), by C. Andrew Barnes and Whiteford, Taylor & Preston, LLP, pursuant to the Federal Rules of Civil Procedure and the Local Rules of the United States District Court for the District of Maryland, hereby sues Defendants White Investments LLC and John Doe Nos. 1-100 (collectively "Defendants") and for its Complaint states as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action against the Defendants White Investments LLC and John Doe Nos. 1-100 who fraudulently effected wire transfers of $2,140,000.00 from Plaintiff's bank account to a bank account held and operated by Defendants by means of unauthorized access to certain email accounts of Plaintiff.

2. Plaintiff seeks to identify and civilly prosecute the person or persons responsible through identification of IP addresses, banking records, and other such information as may lead to the identity of such individual(s) who designed, conspired, or otherwise participated in the thefts and frauds against Plaintiff, and to recover stolen property.

3. Plaintiff will amend this Complaint to allege the true name and capacity of each John Doe Defendant when ascertained. Plaintiff has exercised due diligence and will continue to exercise due diligence to determine Defendants' true names, capacities, and contact information, and to effect service on those Defendants.

4. This is an Action based upon: (1) the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, (2) the Stored Communications Act (18 U.S.C. § 2701(a) and §2707, (3) the Electronic Communications Privacy Act (18 U.S.C. § 2707 and 28 U.S.C. § 1331), and (4) common law actions for Conversion, Trespass to Chattels, and Unjust Enrichment to recover stolen property, seek damages, and enjoin Defendants' malicious and unauthorized access and use of Plaintiff's computer and information systems and emails.

JURISDICTION AND VENUE

5. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, as the action arises under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"), the Stored Communications Act (18 U.S.C. § 2701(a) and §2707(c)), and the Electronic Communications Privacy Act (18 U.S.C. § 2707 and 28 U.S.C. § 1331).

6. This Court has subject-matter jurisdiction under 28 U.S.C. § 1367 over the claims for the common law actions for Conversion, Trespass to Chattels, and Unjust Enrichment, which form part of the same case or controversy as the CFAA claim.

7. This Court has personal jurisdiction over Defendant as a result of the Defendant's unauthorized access into, and misappropriation of information from, a "protected computer" as defined in 18 U.S.C. § 1030(e)(2)(B) since Plaintiff's computers are used in a manner that affects interstate or foreign commerce or communication of the United States.

8. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b). A substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this judicial district. Additionally, a substantial part of the property that is the subject of Plaintiff's claims is situated in this judicial district.

9. This Court may also have diversity jurisdiction over these claims under 28 U.S.C. § 1332(a) because (1) the matter in controversy exceeds the value of $75,000.00 and (2) the controversy is between individuals that are citizens of different jurisdictions, which to date, based upon the locations of banks to which transfers of monies were made and authentications of IP addresses, indicate that Defendant's location is outside of the State of Maryland and that Defendant is a citizen of either Nevada, California (based on locations of banks), or New Jersey, New York, and the District of Columbia (based on IP authentications), or a subject of a foreign state, Russia, England, Japan, Spain, or Germany (also based on IP authentications).

THE PARTIES

10. Plaintiff NABA, Inc. is a nonprofit membership organization dedicated to advancing business leaders in accounting, finance, business, and entrepreneurship. Its office and headquarters are located in Greenbelt, Maryland.

11. On information and belief, White Investments LLC is an active corporation in the State of Arizona with an address of 4747 E. Moreland Street, Phoenix, AZ 85008.

12. On information and belief, Defendants John Doe Nos. 1-100 are persons whose true names, identities, and physical locations are not known at this time.

13. On information and belief, Defendants are responsible for the occurrences herein alleged, and the harms and injuries as herein alleged were proximately caused by such Defendants.

14. Throughout this Complaint, references herein to Defendants are meant to refer to different John Does who, either as individuals or as part of a group, may be identified at a later time.

BACKGROUND AND CHRONOLOGY OF THE FRAUD

15. Defendants executed a phishing-based Man in the Middle Attack ("MitM") to perpetrate the fraud described herein.

16. In a phishing-based MitM attack, a fraudster intercepts communication between two parties, secretly inserting themselves between the user and the service for purposes of monitoring, altering, and redirecting data of its target. Using phishing emails or links, users are redirected to malicious websites controlled by the fraudster, after which time the fraudster can intercept login credentials or other sensitive information. Once login credentials are acquired by the fraudster, the fraudster can receive and send emails from a victim's email account, directing the payment of money to the fraudster before the fraud is discovered.

17. On May 9, 2025, Defendants caused a phishing email to be delivered to a user mailbox at NABA designed to appear like a Federal Express delivery reschedule notice ("First User Account"). The phishing email was designed to appear that it originated from Federal Express and contained a button with a link hosted at https://secure-web.cisco.com.

18. The individual associated with the First User Account provided login credentials to the malicious website via a link contained in the email.

19. Immediately following this event, Microsoft Office 365 registered an anomalous authentication event from Portland, Oregon bearing the user agent string, Axios. Axios is a web/http access tool associated with automated phishing attacks.

20. On or about May 14, 2025, the First User Account was accessed from a Chinese-linked IP address.

21. Beginning May 15, 2025, Defendants, through their control over the First and Second User Accounts (see Second User Account referenced below), effected two fraudulent financial transactions.

22. On May 20, 2025, Defendants, accessing First and Second User Accounts, caused an email to be sent from the First User Account to a second NABA email account ("Second User Account"), directing the second user to have Bank of America ("BOA") make a wire transfer of $870,000.00 for purposes of a purported investment to Defendant White Investments LLC, a limited liability company domiciled in the State of Arizona. The wire transfer was executed and $870,000.00 was sent from Plaintiff's BOA account to a bank account designated by Defendants at the National Bank of Arizona ("NBA").

23. On May 23, 2025, again accessing the First and Second User Accounts, Defendants caused the second user to send a second wire instruction to BOA to transmit via wire $1,270,000.00 to Defendant White Investments LLC. That same day BOA transmitted payment of $1,270,000.00 via wire transfer to Defendant White Investments LLC's account at NBA.

24. At all times relevant to this Complaint, Plaintiff used its computer systems and email to conduct business domestically and abroad, thereby "affecting interstate or foreign commerce or communication." CFAA § 1030(e)(2)(B).

25. To date, Plaintiff has recovered $1,272,800.00 of its funds wired to the National Bank of Arizona, but, upon information and belief, fraudsters retain control of $867,200.00, which amount is sought to be recovered by Plaintiff.

WHITE INVESTMENTS LLC SHOWS IS A SHELL CORPORATION THAT DOES NOT CONDUCT ANY APPARENT LEGITIMATE BUSINESS

26. Upon information and belief, White Investments LLC, while an active corporation in the State of Arizona, is a business that shows no public activity.

27. Upon information and belief, the domain name of White Investments LLC as presented by Defendants, www.whiteinvestmentsllc.com, is a false domain name as it is not a domain registered with ICANN (Internet Center for Assigned Names and Numbers).

28. Upon information and belief, the business address provided by White Investments LLC in its Articles of Organization is not an actual business address, but an address associated with a residential condominium.

29. The phone number provided by Defendants for White Investments LLC has been disconnected.

30. Based upon currently available information, the names of individuals used by Defendants as persons being associated with White Investments LLC, a purported manager, Lene Lynn St. John, and a purported Chief Financial Officer, Timothy McSunas, are either fictious persons or actual persons who have no legal or professional association with White Investments LLC.

REPORTS TO LAW ENFORCEMENT AND FORENSIC ANALYSIS

31. The above fraud was first discovered by Plaintiff on or about May 28, 2025 and immediately reported to federal and state law enforcement agencies.

32. To date, the identities of Defendants are unknown to Plaintiff.

33. Since discovering the incident, Plaintiff acted promptly to secure its computer systems and email account and undertook an investigation to determine the identity of the intruder, the precise scope of the intrusion, and the extent of the damages.

34. In commission of the above, forensic analysis determined that Defendants' access to Plaintiff's computers, information systems, and email accounts was consistent with foreign and domestic IP proxy and VPN activity.

35. Specifically, analysis revealed that IP authentications were connected to California, Oregon, Ohio, Canada, China, Greece, and more.

36. As a result of Defendant's actions, investigation of Plaintiff's computers, information systems, and email applications was required to contain and prevent future harm and to determine the cause and scope of the intrusion.

37. Plaintiff has and will continue to incur additional loss because of forensic costs to investigate and address threat actor activity, methods of unauthorized access/exfiltration, response/containment, and remedial measures necessary to ensure security of Plaintiff's computers, information systems, and email application following Defendant's penetration of same.

38. To date, Plaintiff's loss because of cost and expense of forensic investigation is more than $20,000.00.

FIRST CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030)

39. Plaintiff realleges and incorporates by reference as if fully set forth herein the preceding paragraphs of this Complaint.

40. Defendants in violation of 18 U.S.C. § 1030(a)(4) knowingly and with intent to defraud, accessed a "protected computer" ("used in or affecting interstate or foreign commerce") without authorization from Plaintiff to commit the above stated frauds and obtained things of value aggregating at least $5,000 in a one-year period. 18 U.S.C. § 1030(a)(4).

41. Title 18, United States Code, Section 1030(g) provides that "any person who suffers damage or loss by reason of a violation of the CFAA may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."

42. Defendants' activities constitute a violation of the Federal CFAA, 18 U.S.C.A. § 1030(A)(4) and Plaintiff is entitled to damages under that Act and as pleaded herein, which exceed $5,000.00.

43. Plaintiff is also entitled under the Act to injunctive and equitable relief against Defendant to prevent further and additional violations of the CFAA and other tortious activity.

SECOND CAUSE OF ACTION
Violation of Stored Communications Act

44. Plaintiff re-alleges and incorporates by reference as if fully set forth herein the preceding paragraphs of this Complaint.

45. The Stored Communications Act (hereinafter "SCA") provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," or any person "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

46. At all relevant times, Plaintiff was a user of an electronic communication service as defined by 18 U.S.C. § 2510(15).

47. Defendants, without authorization, intentionally accessed Plaintiff's electronic communications stored by said service.

48. As a result of Defendants' unauthorized access, Plaintiff's electronic communications were obtained, altered, or prevented from being accessed by the Plaintiff, in violation of 18 U.S.C. § 2701(a).

49. Plaintiff has suffered damages as a direct and proximate result of Defendants' actions.

50. Pursuant to 18 U.S.C. § 2707(c), Plaintiff seeks damages for each violation of the SCA, punitive damages, and any other relief the court deems just and proper.

THIRD CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act

51. Plaintiff realleges and incorporates by reference as is fully set forth herein the preceding paragraphs of this Complaint.

52. The Electronic Communications Privacy Act ("ECPA") prohibits the unauthorized interception of the content of any communication through the use of any device and any subsequent disclosure or use of the intercepted contents of any electronic communication. 18 U.S.C. §2511.

53. The ECPA protects both the sending and receipt of communications.

54. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral, or electronic communication is intercepted.

55. Defendants' unlawful actions violated the interception provisions of the ECPA by acquiring and using the contents of Plaintiff's wire and electronic communication through the use of an electronic, mechanical, or other device, in this case computer devices and email applications and systems.

56. As a result of Defendants' actions, Plaintiff's private electronic communications were intercepted, accessed, and utilized in violation of the ECPA.

57. Plaintiff had a reasonable expectation of privacy in these electronic communications.

58. Defendants' unauthorized access has caused harm to the Plaintiff.

FOURTH CAUSE OF ACTION
Conversion

59. Plaintiff realleges and incorporates by reference as if fully set forth herein the preceding paragraphs of this Complaint.

60. Defendants' actions as described above constitute conversion in that Defendants have intentionally and without lawful justification interfered with and assumed control, dominion, or ownership over property of Plaintiff or its principals and has suffered damages.

61. Defendants had no lawful justification to interfere with property of Plaintiff or its principals.

FIFTH CAUSE OF ACTION
Trespass To Chattels

62. Plaintiff realleges and incorporates by reference as if fully set forth herein the preceding paragraphs of this Complaint.

63. Defendants' unauthorized and intentional act of taking and/or damaging the chattel constitutes trespass to chattel.

64. Defendants' actions were without consent or privilege and directly interfered with Plaintiff's possessory rights in chattel.

65. As a result of the Defendants' trespass, Plaintiff has suffered damages in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
Unjust Enrichment

66. Plaintiff realleges and incorporates by reference as if fully set forth herein the preceding paragraphs of this Complaint.

67. By the above unlawful acts, Defendants conferred a benefit to themselves, which Defendants knew of or appreciated such benefit, and Defendants' acceptance or retention of the benefit occurred under such circumstances that it would be inequitable to allow Defendants to retain the benefit without the paying of value in return.

68. Retention of the enrichment is unjust and Plaintiff is harmed in the amounts set forth herein, representing the value of the benefit conferred upon Defendant by Plaintiff.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks this Court to enter judgment against Defendant John Doe Nos. 1-100 and against his, her, or its subsidiaries, affiliates, agents, servants, employees and all persons in active concert or participation with it, granting the following reliefs:

A. Judgment in favor of Plaintiff, and against Defendants, for damages in such amounts as may be proven at trial, but no less than $867,200.00.

B. Disgorgement of any profits realized by Defendants as a result of the violations of law pleaded herein;

C. Punitive or exemplary damages as authorized by law;

D. Interest on damages as proper;

E. Forfeiture of any property, including computer and servers, used to commit the acts described above as authorized by law;

F. Attorneys' fees, costs, and expenses as authorized by law;

G. Injunctive relief enjoining Defendants and any officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with him, from: (i) accessing Plaintiff's computer systems, networks, or data without authorization; destroying or altering Plaintiff's systems, data, or information; (ii) disseminating, selling, or using any data obtained from Plaintiff's computer systems; (iii) engaging in any of the activity complained of herein or from causing any of the injury complained of herein; and (iv) from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

H. Order that Defendants and any officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, immediately deliver to Plaintiff: (i) all copies of the data stolen from Plaintiff's systems; and (ii) all copies of any materials (in paper, electronic, or any other form) that contain or reflect any information derived from Plaintiff's data; and

I. Such other and further relief as this Court or a jury may deem proper and just.

JURY DEMAND

Plaintiff demands a trial by jury on all issues presented in this Complaint.

Respectfully submitted,

/s/ C. Andrew Barnes
C. Andrew Barnes (Bar No. 30561)
WHITEFORD, TAYLOR & PRESTON, LLP
7 Saint Paul Street, Suite 1500
Baltimore, Maryland 21202
Telephone: (410) 347-9484
Facsimile: (410) 234-2234
anbarnes@whitefordlaw.com

-and-

William K. Watanabe (*pro hac vice, admission pending*)
WHITEFORD, TAYLOR & PRESTON, LLP
444 Madison Avenue, 4th Floor
New York, NY 10022
Telephone: (646) 618-6853
Facsimile: (646) 706-5097
kwatanabe@whitefordlaw.com

Attorneys for Plaintiff,
National Association of Black Accountants, Inc.